REMARKS

The Examiner has rejected Claims 13, 14 and 16 under 35 U.S.C. 112, because of insufficient antecedent basis. Applicant emphasizes that such rejection has been avoided by virtue of the clarifications made hereinabove to the claims.

The Examiner has also rejected Claims 1, 6, 7, 8, 13, 14, 16-18, and 20 under 35 U.S.C. 103(a) as being upatentable over Atkinson et al. (U.S. Patent No. 6,367,012B1). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove. Specifically, applicant has incorporated claims 6, 16 and 18 into each of the corresponding independent claims.

With respect to independent Claims 1 and 17, the Examiner has relied on the following excerpts in Atkinson to make a prior art showing of applicant's claimed, "monitoring calls to applications resident on the handheld computer" and "at least temporarily preventing an action requested by said call from being executed if the identified code does not correspond to a code associated with data said action is to be performed upon" (See Claims 1 and 17).

> "A certification or signing method ensures the authenticity and integrity of a computer program, an executable file, or code received over a computer network. The method is used by a publisher or distributor to "sign" an executable file so it can be transmitted with confidence to a recipient over an open network like the Internet. The executable file may be of any executable form, including an executable or portable executable .exe file format, a .cab cabinet file format, an .ocx object control format, or a Java class file.
>
> The code signing method assures the recipient of the identity of the publisher as the source of file (i.e., its authenticity) and that the file has not been modified after being transmitted by the publisher (i.e., the integrity of the file). As a result, the code signing method allows an executable file to be transmitted over open computer networks like the Internet with increased certainty in the identity of the source of the file and minimized risk of contracting a computer virus or other malicious executable computer files." (col. 2, lines 35-52)
>
> "In addition to certifying the identity of the publisher by the name and reputation of the certification agency, dialog 180 provides the recipient of the software with graphical control buttons 182 to selectively elect whether to run the software and links 184 to additional information about the software and the publishing licenses issued by the certification agency. Links 184 allow a software recipient, before deciding to run the received or downloaded code, to obtain additional information about the

> software and the policies or authority under which digital certificate 122 was granted to the publisher who signed the software." (col. 9, lines 9-20)

Applicant asserts that the above excerpts simply disclose certifying "the identity of the publisher by the name and reputation of the certification agency" and allowing "the recipient of the software...to selectively elect whether to run the software..." Simply nowhere does Atkinson even suggest "monitoring calls to applications" and "temporarily preventing an action...from being executed if the identified code does not correspond to a code associated with data said action is to be performed upon." Applicant's claims require an application's creator code to match the creator code of the data it seeks to use, while Atkinson simply requires that the publisher of an application be certified by a certification agency.

Despite this clear distinction and in the spirit of expediting the prosecution of the present application, applicant has amended independent Claims 1 and 17 to read, "at least temporarily preventing an action requested by said call from being executed if the identified creator code does not match a creator code associated with data said action is to be performed upon."

With respect to independent Claims 13 and 20, the Examiner has also relied on both the above and following excerpts from Atkinson to make a prior art showing of applicant's claimed, "monitoring requests for action by applications on the handheld computer" and "wherein evaluating said requests comprises comparing a creator code associated with the application requesting said action with a creator code associated with data the action is to be performed upon" (see independent Claims 13 and 20).

> "This certification of the executable file or code is confirmed or read at the recipient's computer. The public key for the publisher's signature is obtained by decoding or decrypting the digital certificate with the certification agency public key, thereby assuring the authenticity of the software publisher. A cryptographic digest or hash is determined for the code as it is received. The digest is compared to the digest included in the publisher signature. A match between the digests confirms the integrity of the code. A dialog is then rendered by the recipient computer indicating who is providing the code and the certification agency that has authenticated the identity of the publisher." (col. 3, lines 18-24)

Applicant respectfully disagrees that Atkinson discloses "monitoring requests" or "evaluating requests," as claimed by applicant. Atkinson simply teaches "a certification or signing method" that "ensures the authenticity and integrity of a computer program..." by a "cryptographic digest [that] is

determined for the code as it is received [wherein] the digest is compared to the digest included in the publisher signature." Applicant, on the other hand, claims monitoring requests for action by applications, not just certifying the application as a whole. Applicant also claims evaluating the requests by comparing the creator code of the application with the creator code of the data the action is to be performed upon, not comparing a digest associated with the application with a digest included in the publisher signature.

With respect to each of the independent claims, the Examiner has also relied on the above excerpts from Atkinson to make a prior art showing of applicant's claimed, "identifying at least one of the applications as a trusted application, wherein the trusted application is not prevented from performing actions" (see former subject matter of claim 6 and 18, now incorporated into each of the independent claims).

Applicant asserts that the above excerpt from Atkinson in no way even suggests applicant's claimed "trusted applications". Atkinson is simply disclosing certifying an executable file by confirming the integrity of the code and by making sure a certification agency has authenticated the publisher. Atkinson's certification of executable files simply does not meet applicant's claimed "trusted applications" in the way in which applicant claims the same.

For example, applicant claims "wherein at least one of the applications is identified as a trusted application; wherein the trusted application is not prevented from performing actions even if the creator code associated with the trusted application does not match the creator code associated with the data said action is to be performed upon" (see this and similar, but not identical, language in each of the independent claims). This is distinctly different from Atkinson in that applicant claims applications that may be deemed trusted even though their creator code does not match the creator code associated with the data their actions are to be performed upon (i.e. even if a request is identified as potentially harmful).

It is further noted that the Examiner's action is further deficient with respect to applicant's dependent claims. For example, the Examiner has relied on Atkinson's use of a "virtual machine" which allows "possibly malicious code to be executed without fear that it could cause any unauthorized or unwarranted actions" (see col. 2, lines 8-12) to make a prior art showing of

applicant's claimed, "receiving data on an infrared port of the handheld computer and installing said data in a temporary database" (see Claim 7).

Applicant emphasizes that the above "virtual machine" in no way discloses, teaches or even suggests applicant's claimed "installing said data in a temporary database." Atkinson merely discloses a "virtual machine" in which received code can be executed and does not even suggest installing data in a temporary database.

The Examiner has further rejected Claims 9-12 under 35 U.S.C. 103(a) as being unpatentable over Atkinson in view of Chess (U.S. Patent No. 5,572,590). Applicant respectfully disagrees with such rejection.

Specifically, the Examiner relies on Chess's disclosure of "objects to be protected" (col. 1 lines 49-55) et al. to make a prior art showing of applicant's claimed, "wherein the action requested is a password manipulation", "deletion of data", and "manipulation of an operating system" (see Claims 9, 10, and 12). Applicant emphasizes that "objects to be protected" as disclosed in Chess does not rise to the level of specificity of applicant's claimed "password manipulation", "deletion of data", and "manipulation of an operating system". Also, Chess's "objects to be protected" do not even suggest the inclusion of the foregoing claimed features, since Chess is teaching "differentiating legitimate changes in a system from malicious ones" (col. 1, lines 46-48) while applicant claims requests for all actions to manipulate passwords, delete data, or manipulate an operating system.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claim elements, is respectfully requested.

Applicant further brings the Examiner's attention to applicant's added Claims 21-25, which include the following subject matter believed to be novel:

> "wherein the creator code is a 4-byte value used to tie together a plurality of databases related to each application, at least one of the databases is maintained on the handheld computer using a first creator code that is the same as a second creator code associated with a plurality of patches, the at least one database contains a list of a plurality of the creator codes resident on the handheld computer, and each creator code is used to prevent a program from modifying one of the databases with a different creator code" (See Claim 21);
>
> "wherein a user has an options of disabling the detection of potentially harmful actions, specifying whether a plurality of databases scanned by a virus scanner are considered trusted if the virus scanner returns a favorable result, requiring a password to turn the handheld computer on, checking data that has entered the handheld computer through an infra-red (IR) port, protecting passwords, and specifying the trusted application" (See Claim 22);
>
> "wherein the temporary prevention of the action requested by said call involves notifying a user that the potentially harmful action has been requested and giving the user a plurality of options selected from the group consisting of: allowing one of the applications to continue with the action, always allowing one of the applications to perform the action, and preventing one of the applications from performing the action" (see Claim 23 et al);
>
> "wherein the get trap and set trap commands identify a pointer to an original address and replace the original address with a new patch address" (See Claim 24); and

"wherein an efficient detection of viruses is provided for the handheld computer without sacrificing limited memory of the handheld computer" (See Claim 25).

Again, a notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claim elements, is respectfully requested.

All of the independent claims are deemed allowable for the reasons set forth hereinabove. By virtue of their dependence on such claims, the dependent claims are further deemed allowable. Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. For payment of any fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P137_00.123.01).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100